1   Claims:

2   Claim 1

3   A user authentication method, whereby a one-way function

4   F, which should satisfy $v = F(g, -s)$, is determined by

5   employing an integer g that is defined in advance for a

6   relation between a public key v and a secret key s of a

7   prover computer, and whereby a relation is verified

8   between said prover computer and each of multiple

9   verifier computers, comprising the steps of:

10   said prover computer generating a random number a,

11   obtaining a cryptogram A = the function $F(g, a)$, and

12   transmitting said cryptogram A to said verifier

13   computers;

14   said verifier computers generating a random number

15   b, obtaining a cryptogram B = the function $F(g, b)$ and a

16   cryptogram X = the function $F(A, b)$, and transmitting

17   said cryptograms B and X to said prover computer;

18   said prover computer determining whether a relation

19   of said cryptogram X = the function $F(B, a)$ has been

20   established and generating a random number c when said

21   relation has been established, obtaining a cryptogram C

22   = the function $F(g, c)$ and a cryptogram Y = the function

23   $F(B, c)$, or a cryptogram C = the function $F(A, c)$, a

24   cryptogram Y = the function $F(X, c)$ and a cryptogram Z =

25   a function $H(a, Y, s)$, and transmitting said cryptograms

26   C and Y or said cryptograms C, Y and Z to said verifier

27   computers; and

28   said verifier computers, when said cryptogram Y =

29   the function $F(C, b)$ and said cryptogram A = a function

1 J(v, Y, g, Z) are established, determining that said
2 relation between said prover computer and said verifier
3 computer is correct.

4 Claim 2
5 The user authentication method according to claim 1,
6 wherein said public key v is obtained by employing prime
7 numbers p and q that satisfy (q|p - 1), and by defining
8 an element of the order q as said integer g.

9 Claim 3
10 The user authentication method according to claim 1,
11 wherein, by using said public key v and said secret key
12 s, said function F acquires a relation $v = F(g, -s) = g^{-s}$
13 mod p.

14 Claim 4
15 The user authentication method according to claim 1,
16 wherein, when a relation $X = B^a$ mod p is established,
17 said prover computer generates said random number c.

18 Claim 5
19 The user authentication method according to claim 1,
20 wherein said function H has a relation $H(a, Y, s) = a +$
21 Ys mod q.

22 Claim 6
23 The user authentication method according to claim 1,
24 wherein said function J has a relation $J(v, Y, g, Z) =$
25 $v^Y g^Z$ mod p.

1 Claim 7

2 A storage medium on which a user authentication program,

3 which is to be read by a prover computer, is stored

4 whereby a one-way function F, which should satisfy v =

5 $F(g, -s)$, is determined by employing an integer g, which

6 is defined in advance for the relation between a public

7 key v and a secret key s of said prover computer, and

8 whereby a relation is verified between said prover

9 computer and each of multiple verifier computers, said

10 user authentication program permitting said prover

11 computer to perform:

12   a process for generating a random number a and for

13 obtaining a cryptogram A = the function $F(g, a)$, and for

14 transmitting said cryptogram A to said verifier

15 computers;

16   a process for receiving cryptograms B and X from

17 said verifier computer, and for employing said

18 cryptograms to determine whether a relation a cryptogram

19 X = the function $F(B, a)$ has been established;

20   a process for generating a random number c when

21 said relation has been established; and

22   a process for obtaining a cryptogram C = the

23 function $F(g, c)$ and a cryptogram Y = the function $F(B,$

24 $c)$, or a cryptogram C = the function $F(A, c)$, a

25 cryptogram Y = the function $F(X, c)$ and a cryptogram Z =

26 the function $H(a, Y, s)$; and

27   a process for transmitting said cryptograms C and

28 Y, or C, Y and Z, to said verifier computers.

1 Claim 8

2 A storage medium on which a user authentication program,

3 which is to be read by a prover computer, is stored

4 whereby a one-way function F, which should satisfy v =

5 F(g, -s), is determined by employing an integer g, which

6 is defined in advance for the relation between a public

7 key v and a secret key s of said prover computer, and

8 whereby a relation is verified between said prover

9 computer and each of multiple verifier computers, said

10 user authentication program permitting said verifier

11 computers to perform:

12   a process for receiving a cryptogram A from said

13 prover computer and for generating a random number b;

14   a process for obtaining a cryptogram B = the

15 function F(g, b) and a cryptogram X = the function F(A,

16 b), using said random number b and said cryptogram that

17 is received, and for transmitting said cryptograms B and

18 X to said prover computer;

19   a process for receiving, from said prover computer,

20 a cryptogram C = the function F(g, c) and a cryptogram Y

21 = the function F(B, c), or a cryptogram C = the function

22 F(A, c), a cryptogram Y = the function F(X, c) and a

23 cryptogram Z = the function H(a, Y, s); and

24   a process, based on said cryptograms C and Y or C,

25 Y and Z that are received, for verifying a relation

26 between said verifier computer and said prover computer

27 when two relations of said cryptogram Y = the function

28 F(C, b) and said cryptogram A = the function J(v, Y, g,

29 Z) are established at the same time.

1 Claim 9

2 A user authentication apparatus for a prover computer,

3 wherein a one-way function F, which should satisfy $v =$

4 $F(g, -s)$, is determined by employing an integer g, which

5 is defined in advance, for a relation between a public

6 key v and a secret key s of said prover computer, and

7 wherein a relation is verified between said prover

8 computer and each of multiple verifier computers, said

9 user authentication apparatus comprising:

10 transmission means, for generating a random number

11 a and obtaining a cryptogram $A =$ the function $F(g, a)$,

12 and for transmitting said obtained cryptogram A to said

13 verifier computers;

14 reception means, for receiving cryptograms B and X

15 from said verifier computers;

16 verification means, for employing said cryptograms

17 B and X to determine whether a relation of said

18 cryptogram $X =$ the function $F(B, a)$ has been

19 established;

20 cryptogram computation means, for generating a

21 random number c when it has been ascertained that said

22 relation has been established, and for obtaining a

23 cryptogram $C =$ the function $F(g, c)$ and a cryptogram $Y =$

24 the function $F(B, c)$, or a cryptogram $C =$ the function

25 $F(A, c)$, a cryptogram $Y =$ the function $F(X, c)$ and a

26 cryptogram $Z =$ the function $H(a, Y, s)$; and

27 cryptogram transmission means, for transmitting

28 said cryptograms C and Y or C, Y and Z to said verifier

29 computers.

1   Claim 10

2   A user authentication apparatus for a prover computer

3   wherein a one-way function F, which should satisfy $v =$

4     $F(g, -s)$, is determined by employing an integer g, which

5   is defined in advance, for the relation between a public

6   key v and a secret key s of a prover computer, and

7   wherein a relation is verified between said prover

8   computer and each of multiple verifier computers, said

9   user authentication apparatus comprising:

10   reception means, for receiving a cryptogram A from

11   said prover computer;

12   transmission means, for generating a random number

13   b, and for employing said random number b and said

14   cryptogram A that is received to obtain a cryptogram $B =$

15   the function $F(g, b)$ and a cryptogram $X =$ the function

16     $F(A, b)$, and for transmitting said cryptograms B and X

17   to said prover computer;

18   cryptogram reception means, for receiving from said

19   prover computer a cryptogram $C =$ the function $F(g, c)$

20   and a cryptogram $Y =$ the function $F(B, c)$ or a

21   cryptogram $C =$ the function $F(A, c)$, a cryptogram $Y =$

22   the function $F(X, c)$, and a cryptogram $Z =$ the function

23     $H(a, Y, s)$; and

24   verification means, for performing a procedure,

25   based on said cryptograms C, Y and Z that are received,

26   for verifying a relation between said verifier computers

27   and said prover computer when two relations of said

28   cryptogram $Y =$ the function $F(C, b)$ and said cryptogram

29     $A =$ the function $J(v, Y, g, Z)$ are established at the

30   same time.

1   Claim 11

2   A user authentication system comprising:

3   the user authentication apparatus for said prover

4   computer according to claim 9; and

5   a plurality of user authentication apparatuses for

6   said verifier computers according to claim 10.

7   Claim 12

8   A user authentication system, wherein a one-way function

9   F, which should satisfy $v = F(g, -s)$, is determined by

10   employing an integer g, which is defined in advance, for

11   the relation between a public key v and a secret key s

12   of a prover computer, and wherein a relation is verified

13   between said prover computer and each of multiple

14   verifier computers, comprising:

15   transmission means, for said prover computer, for

16   generating a random number a and obtaining a cryptogram

17   $A =$ the function $F(g, a)$, and for transmitting said

18   obtained cryptogram A to said verifier computers;

19   reception means for said verifier computers, for

20   receiving said cryptogram A from said prover computer;

21   transmission means for said verifier computers, for

22   generating a random number b with which said cryptogram

23   A is employed to obtain a cryptogram $B =$ the function

24   $F(g, b)$ and a cryptogram $X =$ the function $F(A, b)$, and

25   for transmitting said cryptograms B and X to said prover

26   computer;

27   reception means for said prover computer, for

28   receiving said cryptograms B and X from said verifier

1   computers;

2   verification means for said prover computer, for

3   employing said cryptograms B and X to determine whether

4   a relation of said cryptogram X = the function F(B, a)

5   has been established;

6   cryptogram computation means for said prover

7   computer, for generating a random number c when it is

8   ascertained that said relation has been established, and

9   for obtaining said cryptogram C = the function F(g, c)

10   and said cryptogram Y = the function F(B, c), or said

11   cryptogram C = the function F(A, c) and said cryptogram

12   Y = the function F(X, c), and a cryptogram Z = the

13   function H(a, Y, s); and

14   cryptogram transmission means for said prover

15   computer, for transmitting said cryptograms C, Y and Z

16   to said verifier computers;

17   cryptogram reception means, for said verifier

18   computers, for receiving said cryptograms C, Y and Z

19   from said prover computer; and

20   verification means for said verifier computers, for

21   employing said cryptograms C, Y and Z that are received

22   to verify a relation between said verifier computers and

23   said prover computer when two relations of said

24   cryptogram Y = the function F(C, b) and said cryptogram

25   A = the function J(v, Y, g, Z) are established at the

26   same time.

27   13. A computer program product comprising a computer

28   usable medium having computer readable program code means

29   embodied therein for causing user authentication, the

1   computer readable program code means in said computer

2   program product comprising computer readable program code

3   means for causing a computer to effect the apparatus of

4   claim 9.

5   14.   A computer program product comprising a computer

6   usable medium having computer readable program code means

7   embodied therein for causing user authentication, the

8   computer readable program code means in said computer

9   program product comprising computer readable program code

10   means for causing a computer to effect the apparatus of

11   claim 10.

12   15.   A computer program product comprising a computer

13   usable medium having computer readable program code means

14   embodied therein for causing user authentication, the

15   computer readable program code means in said computer

16   program product comprising computer readable program code

17   means for causing a computer to effect the system of

18   claim 11.

19   16.   A computer program product comprising a computer

20   usable medium having computer readable program code means

21   embodied therein for causing user authentication, the

22   computer readable program code means in said computer

23   program product comprising computer readable program code

24   means for causing a computer to effect the system of

25   claim 12.

26   17.   An article of manufacture comprising a computer

1   usable medium having computer readable program code means
2   embodied therein for implementing a user authentication
3   method, the computer readable program code means in said
4   article of manufacture comprising computer readable
5   program code means for causing a computer to effect the
6   steps of claim 1.